

US Department of Education Federal Student Aid



Password Parameters Policy & Procedures

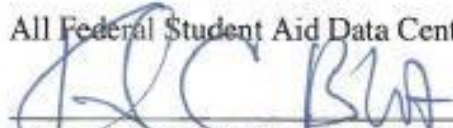
July 6, 2006

Federal Student Aid CIO: IT Security 2-03

Page 1 of 22

Distribution: All Federal Student Aid Data Centers and Applications

Approved by:


Katie Blot, Federal Student Aid Chief Information Officer


Date

Table of Contents

| | | |
|-----------|---|-----------|
| 1 | OBJECTIVES | 4 |
| 2 | SCOPE | 4 |
| 3 | POLICY | 4 |
| 4 | EXCEPTIONS | 6 |
| 5 | PROCEDURES..... | 7 |
| 6 | ROLES & RESPONSIBILITIES..... | 7 |
| 7 | DEFINITIONS..... | 8 |
| 8 | ENFORCEMENT | 9 |
| 9 | POINT OF CONTACT | 9 |
| 10 | AUTHORITY..... | 9 |
| 11 | LOCATION..... | 10 |
| 12 | EFFECTIVE DATE | 10 |
| 13 | REVIEW SCHEDULE..... | 10 |
| | ATTACHMENT A: PASSWORD PARAMETER SETTINGS BY OPERATING ENVIRONMENT | 11 |
| | ATTACHMENT B: PASSWORD PARAMETER COMPLIANCE MATRIX | 21 |
| | ATTACHMENT C: TABLE OF APPLICABLE RISK ASSESSMENT FORMS | 23 |

Document Revision History

This page summarizes the document revision history. Each entry includes the version number for the document itself, the date of the change, the page(s) numbers where the changes occurred, and a (very) brief description of the change. The most current change will always appear on the first row of the table.

Any changes/updates to the document will be provided in detail in the Document Revision History table and will be distributed to those appropriate individuals by change pages for hard copy distribution, once baselined and under change control. Revision bars on the left-hand side of the page will reflect the line(s) where a change has occurred. Complete the page number column only if minor changes are made. If the document is undergoing a complete revision, this field can be marked N/A.

| Revision Number | Date of Change | Section(s) Affected | Brief Description of Change |
|-----------------|----------------|----------------------|--|
| 1.0 | 2006-3-31 | | Initial Draft Document Release Date |
| 1.1 | 2006-4-14 | 2-7, Att A, Att B | Updates per comments from Bob Ingwalson |
| 1.2 | 2006-5-5 | 3, Att C | Added service account section, attachment of password-related RAFs |
| 1.3 | 2006-6-21 | 2,3,5,7, Att A, B, C | Added policy clarifications, definition clarifications, RAF table |
| | | | |

1 OBJECTIVES

Passwords play a vital role in the prevention of unauthorized access into a system. The most common of authentication mechanisms, passwords help control entry into Federal Student Aid systems. The effectiveness of this control, however, depends on the strength of the password and the stringency at which Federal Student Aid protects it. Training on proper password protection, and secure password issuance and resetting procedures provide important operational controls; the password parameter settings put in place within each system provide the necessary technical controls. This policy document supplements the Department of Education Handbook OCIO -01, *Handbook for Information Assurance Policy* and provides the Federal Student Aid required password parameter settings.

2 SCOPE

This document applies to all Federal Student Aid information technology components, including those components operated by Federal Student Aid contractors, requiring user identification and authentication controls. The policy and procedures cover the settings and maintenance of password parameters for all security authorities in use by Federal Student Aid systems for the authentication of users, administrators, or machine-to-machine interfaces between systems.

3 POLICY

All Federal Student Aid systems shall comply with the applicable password parameter settings as described in this document. Specific application parameter settings (e.g. Windows, RACF, Oracle) can be found in Attachment A. These setting values are in accordance with Federal and Departmental guidance, and follow industry best practices. Systems are responsible for providing supporting countermeasures to cover for missing parameter settings. Some exceptions have already been identified and documented in Risk Analysis Forms (RAFs). Attachment C contains a list of these exceptions and applicable RAFs. Otherwise, system owners will need to document any noncompliance with parameter settings as an accepted risk.

3.1. User Account Parameters

User accounts refer to all accounts established within Federal Student Aid systems used by Federal Student Aid employees, system administrators, partners or customers (for example, students or parents). Whether established automatically by the system or manually by an administrator, these accounts must have their account password parameters, at a minimum, set to the following, as identified in Table 3-1:

| Parameter | Setting |
|-----------|---------|
|-----------|---------|

| Parameter | Setting |
|---|--|
| Complexity | Systems shall enable automatic verification of passwords by the system. Passwords must contain three of the four following criteria: <ul style="list-style-type: none"> English uppercase letters (A-Z) English lowercase letters (a-z) Westernized Arabic numerals (0-9) Non-alphanumeric special characters (!, @, #, \$, &, *) |
| Minimum password length | Eight (8) characters |
| Expiration date | 90 days (90 days minus grace period if grace period is available) |
| Grace period (if available) | 0-5 days |
| Maximum number of consecutive unsuccessful login attempts | After three (3) unsuccessful login attempts in a row, the account shall be locked |
| Lockout duration * | 30 minutes |
| Minimum password age ** | 5 days |
| Password reuse | Users may not use their previous five (5) passwords, <u>or</u> Users may not reuse a password within the past year |
| Unauthorized passwords | Users may not choose a password that matches or resembles the word “password” in any form (e.g. capitalized, adding a number) Users may not choose a password that pertains in any way to their name in any form (e.g. login name, first or last name) |
| Inactive accounts disabling | Accounts showing no activity shall be disabled after 90 days. If no automated capability is available, manual methods shall be implemented and identified in the System Security Plan |

* If and only if a system is incapable of setting lockout duration, it is acceptable to indefinitely lock a user account until rest by an administrator. However, if this feature is available, lockout duration shall be set at 30 minutes (or as close to 30 minutes as possible).

** Administrators may reset passwords less than five days of age if necessary (e.g. compromised or forgotten). If minimum age capability is not available, an authorized alternative is to set Password Reuse to either “Users may not use their previous twenty (20) passwords,” or “Users may not reuse a password within the past year”

Table 3-1 – User Account Parameter Settings

3.2. Service Account Parameters

Service accounts refer to those non-interactive accounts required by a system in order for that system to function properly. These could be used externally by two systems or subsystems to pass information, or internally by the application to perform specific administrative functions. **No person shall log into a system using these accounts**, and systems should limit the ability of users to use these accounts, whether by not allowing users to log-in locally using the account, or denying access to the Graphical User Interface. All service accounts must have their account password parameters, at a minimum, set to the following, as identified in Table 3-2:

| Parameter | Setting |
|---|--|
| Complexity | Systems shall enable automatic verification of passwords by the system. Passwords must contain three of the four following criteria: <ul style="list-style-type: none"> English uppercase letters (A-Z) English lowercase letters (a-z) Westernized Arabic numerals (0-9) Non-alphanumeric special characters (!, @, #, \$, &, *) |
| Minimum password length | Eight (8) characters |
| * Expiration date | 90 days if changed automatically; one (1) year if changed manually |
| * Grace period (if available) | 0 days |
| * Maximum number of consecutive unsuccessful login attempts | After three (3) unsuccessful login attempts in a row, system administrators are alerted; however, accounts are not locked. |
| * Lockout duration | Not used – accounts not locked after unsuccessful |
| ** Minimum password age | 5 days |
| Password reuse | Users may not use their previous five (5) passwords, <u>or</u> Users may not reuse a password within the past year |
| Unauthorized passwords | Users may not choose a password that matches or resembles the word “password” in any form (e.g. capitalized, adding a number) Users may not choose a password that pertains in any way to their name in any form (e.g. login name, first or last name) |

* Service Account parameter settings different from User Account

** Administrators may reset passwords less than five days of age if necessary (e.g. compromised or forgotten). If minimum age capability is not available, an authorized alternative is to set Password Reuse to either “Users may not use their previous twenty (20) passwords,” or “Users may not reuse a password within the past year”

Table 3-2 – Service Account Parameter Settings

4 EXCEPTIONS

No portion of the *Federal Student Aid Password Parameter Policy* can be waived. However, a business unit can maintain non-compliance with a portion of this policy if the business unit has made a risk based decision not to comply, and the Designated Approving Authority (DAA) approves that decision. The DAA for Federal Student Aid is its Chief Operating Officer.

The business decision not to comply with this policy shall be based on:

- Other controls (technical or procedural) that limit the risk substantially enough to make the additional control required by this policy needless
- The risk the policy aims to minimize is already substantially remote
- The cost of implementing the policy is not commensurate with the protection offered by the policy
- The implementation of the policy will break or degrade system functionality
- The implementation of the policy will impose greater risks upon the system

A Department of Education Risk Analysis Form (RAF) must support each decision and clearly identify the following:

- Policy that is not being met
- Impact level
- Existing controls
- Threat level
- Likelihood of compromise
- Overall risk
- Justification for accepting the risk

Should a business decision be made to not comply with the policy, steps must be taken to reduce those risks to an acceptable level, update the System Security Plan, and maintain a satisfactory level of protection.

5 PROCEDURES

System developers and administrators shall implement all of the password policies that the operating system or application is physically capable of handling. However, it is understood that not all operating systems and applications possess the capability of implementing all of the parameters set above. In such cases, appropriate complementary countermeasures must be put in place to mitigate the risk of non-compliance with the entirety of the Password Parameter policies. See Attachment A for implementation guidance for various operating systems and applications. This guidance is not inclusive of all technologies or versions; if not listed, it is expected that system owners shall determine how to implement Federal Student Aid policies.

System administrators will review parameter settings on all account types (user, administrator, machine-to-machine) at least annually to verify compliance with policy and/or update parameter settings. If the operating system is incapable of automatically verifying complexity and age of passwords, administrators shall conduct scans every ninety days to determine non-compliant passwords. If capable, Federal Student Aid systems will use automatic, real time password validation mechanisms. See Attachment B for a password parameter compliance capabilities matrix.

6 ROLES & RESPONSIBILITIES

Chief Security Officer is responsible for:

- Oversight of the implementation and validation of these policies

System Managers are responsible for:

- Ensuring that password parameters have been properly implemented.
- Ensuring that validation activities take place on at least an annual basis.
- Responsibilities pertaining to the EXCEPTION process:

- Obtaining approval from the Designated Approving Authority prior to implementing exceptions.
- Informing all interconnected Major Applications of the accepted risk.
- Ensuring that risks have been analyzed and appropriately mitigated prior to implementation.

System Security Officers are responsible for:

- Working directly with the Contractor to ensure proper implementation of password parameters.
- Responsibilities following the EXCEPTION process:
 - Determining the risk level of possible exceptions, and their related mitigation strategies.
 - Working directly with the Contractor to ensure the approved mitigation strategy is properly implemented.
- Maintaining the System Security Plan with all password parameter settings and related security controls.

System Operations Contractors are responsible for:

- Implementing the policies to apply to all accounts, including users, administrators, and machine-to-machine accounts.
- If necessary, providing the System Security Officer with quarterly assessment reports from the results of password vulnerability scans.
- Identifying possible policy exceptions to the System Security Officer.

7 DEFINITIONS

Lockout Duration – The period of time an account will be locked after repeated unsuccessful login attempts before automatically unlocked.

Minimum Age – The minimum number of days a password must be in use before the user may change it. This prevents users from quickly rolling through passwords in order to use a favored password repeatedly. Note that this is a parameter setting enforced upon users; administrators may force a password change in case of such cases as compromised or forgotten passwords.

Password Complexity – The practice of expanding the set of possible characters used within a password from the 26 letters of the alphabet to one including upper and lowercase letters, numbers, and/or special characters.

Password Expiration – The maximum period during which a password remains valid. After expiration, the user must change the password else the account will become locked.

Password Grace Period – The period of time after password expiration during which the user, after his or her first successful login, must change the password. For example, suppose a system is set such that a password expires in 85 days and has a five-day grace period. If a user's password expires on day 85, but the user does not log in, the account will not be locked. If the user then logs

in on day 92, the user will then have a five-day grace period during which to change their password, else the account will be locked on day 97.

Password Reuse – The ability to use a previously used password when entering a new password.

Security Authority – The software entity that enforces identification and authentication for a given system or application.

8 ENFORCEMENT

Violation of this policy could result in loss of, or limitations on use of information resources, as well as disciplinary and/or legal action, including termination of employment or referral for criminal prosecution.

9 POINT OF CONTACT

Federal Student Aid OCIO Chief Security Officer (CSO)

10 AUTHORITY

- Federal Student Aid Information Technology Security and Privacy Policy
- Department of Education Handbook OCIO -01, *Handbook for Information Assurance Policy*
- Federal Information Security Management Act of 2002 (FISMA), PL 107-347, December 17, 2002
- OMB Circular A-130, *Management of Federal Information Resources, Appendix III, Security of Federal Automated Information Resources*, November 28, 2000.
- FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems*
- NIST Special Publication 800-26, *Security Self-Assessment Guide for Information Technology Systems*
- NIST Special Publication 800-53, *Recommended Security Controls for Federal Information Systems*
- NIST Special Publication 800-63, *Electronic Authentication Guideline: Recommendations of the National Institute of Standards and Technology*

11 LOCATION

All Federal Student Aid security policies are located on the Online Security Center (OSC) at the following URL: http://fsanet/cio/products/it_security_portal/

12 EFFECTIVE DATE

July 6, 2006

13 REVIEW SCHEDULE

This policy should be reviewed and updated annually.

Latest Review Date: July 6, 2006

ATTACHMENT A: Password Parameter Settings by Operating Environment

This Page Intentionally Left Blank

Password Parameter Settings by Operating Environment

The following procedures describe the parameter names and values for password settings across multiple operating environments. System developers and administrators must ensure that these settings are implemented and maintained for all accounts, including user, administrator, and machine-to-machine interfaces. This guidance is not inclusive of all technologies or versions; if not listed, it is expected that system owners shall determine how to implement Federal Student Aid policies.

In some cases, the capability of exactly setting a parameter per Federal Student Aid policy is not supported by the operating environment. In these cases, parameters should be set as close to policy as possible. If the operating environment is wholly incapable of supporting the policy, this should be documented as an accepted risk.

A.1 Windows Versions: NT Server 4.0, 2000, Server 2003

| Parameter / Policy | Setting |
|---|--|
| Complexity: Systems shall enable automatic verification of passwords by the system. Passwords must contain three of the four following criteria: <ul style="list-style-type: none">English uppercase letters (A-Z)English lowercase letters (a-z)Westernized Arabic numerals (0-9)Non-alphanumeric special characters (!, @, #, \$, &, *) | Enable <u>Passwords must meet complexity requirements</u> (Requires three of the following five categories: English uppercase characters (A - Z); English lowercase characters (a - z); base 10 digits (0 - 9); non " alphanumeric (For example: !, \$, #, or %); Unicode characters.) |
| Minimum password length: Eight (8) characters | Set <u>Minimum Password Length</u> to 8 characters |
| Expiration date: 90 days (85 days if grace period is available) | Set <u>Maximum Password Age</u> to 90 |
| Grace period: (if available) 5 days | Not available |
| Maximum number of consecutive unsuccessful login attempts: After three (3) unsuccessful login attempts in a row, the account shall be locked | Set <u>LockoutThreshold</u> to 3 |
| Lockout Duration: 30 minutes | Set <u>LockoutDuration</u> to 30 Set <u>Reset account lockout counter after</u> to 30 (Resets bad login attempt counter after 30 minutes) Set <u>ForceUnlockLogon</u> to 0 (Does not allow use of cached passwords to login immediately after unlocking an account) |
| Minimum password age: 5 days | Set <u>Minimum Password Age</u> to 5 |
| Password reuse: Users may not use their previous five (5) passwords Users may not reuse a password within the past year | Set <u>Enforce Password History</u> to 5 |

| Parameter / Policy | Setting |
|---|---|
| Unauthorized passwords: Users may not choose a password that matches or resembles the word “password” in any form (e.g. capitalized, adding a number) Users may not choose a password that pertains in any way to their name in any form (e.g. login name, first or last name) Password uniqueness must be maintained (no use of near-identical passwords) | Enable Passwords must meet complexity requirements (Will not allow passwords to contain three or more characters from the user's account name. If the account name is less than three characters long then this check is not performed because the rate at which passwords would be rejected would be too high.) |
| Inactive accounts disabling: Accounts showing no activity shall be disabled 90 days following password expiration. | Not available – must be reviewed manually |

A.2 UNIX RACF Versions: 1.7 and higher

| Parameter / Policy | Setting |
|--|--|
| Complexity: Systems shall enable automatic verification of passwords by the system. Passwords must contain three of the four following criteria: <ul style="list-style-type: none"> English uppercase letters (A-Z) English lowercase letters (a-z) Westernized Arabic numerals (0-9) Non-alphanumeric special characters (!, @, #, \$, &, *) | Set support for mixed (upper/lower) case: SETROPTS PASSWORD (MIXEDCASE) Set support for alphanumeric, including #, \$, @ SETROPTS PASSWORD (RULE1 (LENGTH(8) ALPHANUM(1:8)) (Requires at least one alphabetic or national character (#, \$, @) and one numeric character.) Enforce of three characteristics not available |
| Minimum password length: Eight (8) characters | Included within: SETROPTS PASSWORD (RULE1 (LENGTH(8) ALPHANUM(1:8)) |
| Expiration date: 90 days (85 days if grace period is available) | Set total lifespan (expiration + grace period) of password to 90 SETROPTS PASSWORD (INTERVAL(90)) |
| Grace period: (if available) 5 days | Not available |
| Maximum number of consecutive unsuccessful login attempts: After three (3) unsuccessful login attempts in a row, the account shall be locked | Revokes access after three unsuccessful login attempts in a row (NOTE: revocation occurs upon users next login attempt): SETROPTS PASSWORD (REVOKE(3)) Must also set: SETROPTS INITSTATS |
| Lockout Duration: 30 minutes | Not available – accounts must be locked indefinitely until an administrator unlocks the account |
| Minimum password age: 5 days | SETROPTS PASSWORD (MINCHANGE (5)) |
| Password reuse: Users may not use their previous five (5) passwords Users may not reuse a password within the past year | Users may not use their previous five (5) passwords SETROPTS PASSWORD (HISTORY(5)) Must also set: SETROPTS INITSTATS Not capable of comparing to one year of passwords |
| Unauthorized passwords: Users may not choose a password that matches or resembles the word “password” in any form (e.g. capitalized, adding a number) Users may not choose a password that pertains in any way to their name in any form (e.g. login name, first or last name) Password uniqueness must be maintained (no use of near-identical passwords) | Not available |

| Parameter / Policy | Setting |
|---|--|
| Inactive accounts disabling: Accounts showing no activity shall be disabled 90 days following password expiration. | Revoke access on accounts showing no activity over 90 days: SETROPS INACTIVE (90) Must also set: SETROPTS INITSTATS |

A.3 Oracle Database Versions: 8i, 9i, 10g

| Parameter / Policy | Setting |
|--|--|
| Complexity: Systems shall enable automatic verification of passwords by the system. Passwords must contain three of the four following criteria: <ul style="list-style-type: none"> English uppercase letters (A-Z) English lowercase letters (a-z) Westernized Arabic numerals (0-9) Non-alphanumeric special characters (!, @, #, \$, &, *) | Set password_verify_function to a verification function (using Perl or SQL) enforcing required policies Can enforce alphanumeric and special characters, and Oracle Database will differentiate case sensitivity. |
| Minimum password length: Eight (8) characters | Set password_verify_function to a verification function (using Perl or SQL) enforcing required length |
| Expiration date: 90 days (85 days if grace period is available) | In Database profile: password_life_time=85 |
| Grace period: (if available) 5 days | In Database profile password_grace_time=5 |
| Maximum number of consecutive unsuccessful login attempts: After three (3) unsuccessful login attempts in a row, the account shall be locked | In Database profile: failed_login_attempts=3 |
| Lockout Duration: 30 minutes | password_lock_time=1 (minimum time is 1 day) |
| Minimum password age: 5 days | Not available – Password reuse must either be set to one year, or a history of 20 passwords |
| Password reuse: Users may not use their previous five (5) passwords Users may not reuse a password within the past year | <u>Preferred:</u> Users may not reuse a password within the past year In Database profile: password_reuse_time= 365 -or (cannot use both)- Users may not use their previous five (20) passwords (see minimum password age): In Database profile: password_reuse_max=20 When setting one of these profiles, the other <u>must</u> be set to “Unlimited” |
| Unauthorized passwords: Users may not choose a password that matches or resembles the word “password” in any form (e.g. capitalized, adding a number) Users may not choose a password that pertains in any way to their name in any form (e.g. login name, first or last name) Password uniqueness must be maintained (no use of near-identical passwords) | Set password_verify_function to a verification function (using Perl or SQL) enforcing required policies |

| Parameter / Policy | Setting |
|---|---|
| Inactive accounts disabling: Accounts showing no activity shall be disabled 90 days following password expiration. | Not available – must be reviewed manually |

Note: Oracle’s default password verification function (utlpwdmg.sql) checks for the following:

- The password has a minimum length of 4.
- The password is not the same as the userid.
- The password has at least one alpha, one numeric, and one punctuation character.
- The password does not match simple words like welcome, account, database, or user.
- The password differs from the previous password by at least 3 letters.

At a minimum, this function must be changed to only allow a minimum length of eight characters, and preferably would also include additional unauthorized passwords such as “p@ssword1”, “pa\$\$word1”, etc.

A.4 Oracle Applications Versions: 11i

| Parameter / Policy | Setting |
|--|--|
| Complexity: Systems shall enable automatic verification of passwords by the system. Passwords must contain three of the four following criteria: <ul style="list-style-type: none"> • English uppercase letters (A-Z) • English lowercase letters (a-z) • Westernized Arabic numerals (0-9) • Non-alphanumeric special characters (!, @, #, \$, &, *) | Set password_verify_function to a verification function (using Perl or SQL) enforcing required policies Can enforce alphanumeric and special characters; Oracle Applications will not differentiate between upper and lowercase (everything read as uppercase). |
| Minimum password length: Eight (8) characters | <u>Signon Password Length</u> = 8 |
| Expiration date: 90 days (85 days if grace period is available) | <u>Expiration Date Parameter</u> = 90 |
| Grace period: (if available) 5 days | Not available |
| Maximum number of consecutive unsuccessful login attempts: After three (3) unsuccessful login attempts in a row, the account shall be locked | <u>Signon Password Failure Limit</u> = 3 |
| Lockout Duration: 30 minutes | Not available – accounts must be locked indefinitely until an administrator unlocks the account |
| Minimum password age: 5 days | Not available – password reuse must be set to one year |
| Password reuse: Users may not use their previous five (5) passwords Users may not reuse a password within the past year | <u>Signon Password No Reuse</u> = 365 |

| Parameter / Policy | Setting |
|---|---|
| Unauthorized passwords: Users may not choose a password that matches or resembles the word "password" in any form (e.g. capitalized, adding a number) Users may not choose a password that pertains in any way to their name in any form (e.g. login name, first or last name) Password uniqueness must be maintained (no use of near-identical passwords) | Signon Password Hard to Guess = Yes Implements the following controls: <ul style="list-style-type: none"> The password contains at least one letter and at least one number. The password does not contain the username. The password does not contain repeating characters. |
| Inactive accounts disabling: Accounts showing no activity shall be disabled 90 days following password expiration. | Not available – must be reviewed manually |

A.5 Solaris Versions: 9

| Parameter / Policy | Setting |
|--|---|
| Complexity: Systems shall enable automatic verification of passwords by the system. Passwords must contain three of the four following criteria: <ul style="list-style-type: none"> English uppercase letters (A-Z) English lowercase letters (a-z) Westernized Arabic numerals (0-9) Non-alphanumeric special characters (!, @, #, \$, &, *) | By default, Solaris requires that each password must contain at least two alphabetic characters and at least one numeric or special character. In this case, "alphabetic" refers to all upper or lower case letters. Does not enforce three characteristics Solaris by default compares passwords to the requirements set in the etc/default/passwd file. |
| Minimum password length: Eight (8) characters | <pre>logins -ox awk -F: '(\$1 == "root" \$8 == "LK") { next } { \$cmd = "passwd" } (\$11 <= 0 \$11 > 91) { \$cmd = \$cmd " -x 91" } (\$10 < 7) { \$cmd = \$cmd " -n 7" } (\$12 < 7) { \$cmd = \$cmd " -w 7" } (\$cmd != "passwd") { print \$cmd " " \$1 }\' > /etc/CISupd_accounts /sbin/sh /etc/CISupd_accounts rm -f /etc/CISupd_accounts cat <<EO_DefPass >/etc/default/passwd MAXWEEKS=13 MINWEEKS=1 WARNWEEKS=1 PASSLENGTH=8 EO_DefPass</pre> |
| Expiration date: 90 days (85 days if grace period is available) | See Minimum Password Length. Expiration is set at 13 weeks, or 91 days (settings are in number of weeks, preventing exactly 90 day expiration) |
| Grace period: (if available) 5 days | Not available |
| Maximum number of consecutive unsuccessful login attempts: After three (3) unsuccessful login attempts in a row, the account shall be locked | Edit /etc/default/login with RETRIES=3 |
| Lockout Duration: 30 minutes | Not available – accounts must be locked indefinitely until an administrator unlocks the account |
| Minimum password age: 5 days | See Minimum Password Length. Settings are in weeks, so a one week minimum is the smallest interval. |

| Parameter / Policy | Setting |
|---|---|
| Password reuse: Users may not use their previous five (5) passwords Users may not reuse a password within the past year | # grep "^HISTORY=" /etc/default/passwd HISTORY=5 Note: Only available for Solaris 10. No support available to limit password reuse per a set time period. |
| Unauthorized passwords: Users may not choose a password that matches or resembles the word "password" in any form (e.g. capitalized, adding a number) Users may not choose a password that pertains in any way to their name in any form (e.g. login name, first or last name) Password uniqueness must be maintained (no use of near-identical passwords) | By default, Solaris has the following limitations on password selection: <ul style="list-style-type: none"> Each password must differ from the user's login <i>name</i> and any reverse or circular shift of that login <i>name</i>. For comparison purposes, an upper case letter and its corresponding lower case letter are equivalent. New passwords must differ from the old by at least three characters. For comparison purposes, an upper case letter and its corresponding lower case letter are equivalent. |
| Inactive accounts disabling: Accounts showing no activity shall be disabled 90 days following password expiration. | Usermod -f 90 <userid> Where <userid> is replaced with the account usernames. This expires idle accounts after 30 days of inactivity. |

A.6 Tivoli Identity Manager (IBM) Versions: 4.6

| Parameter / Policy | Setting |
|--|---|
| Complexity: Systems shall enable automatic verification of passwords by the system. Passwords must contain three of the four following criteria: <ul style="list-style-type: none"> English uppercase letters (A-Z) English lowercase letters (a-z) Westernized Arabic numerals (0-9) Non-alphanumeric special characters (!, @, #, \$, &, *) | Set <u>Minimum Alphabetic Characters Required</u> to 1 Set <u>Minimum Numeric Characters Required</u> to 1 Check <u>Disallow In Dictionary?</u> Add "password" variants to password dictionary |
| Minimum password length: Eight (8) characters | Set <u>Minimum Length</u> to 8 |
| Expiration date: 90 days (85 days if grace period is available) | Set <u>Password Expiration Period</u> to 90 |
| Grace period: (if available) 5 days | Not available |
| Maximum number of consecutive unsuccessful login attempts: After three (3) unsuccessful login attempts in a row, the account shall be locked | Set <u>Maximum Number Of Invalid Logon Attempts</u> to 3 |
| Lockout Duration: 30 minutes | Not available – accounts must be locked indefinitely until an administrator unlocks the account |
| Minimum password age: 5 days | Not available – Password reuse must either be set to a history of 20 passwords |
| Password reuse: Users may not use their previous five (5) passwords Users may not reuse a password within the past year | Set <u>Repeated History Length</u> to 20 |

| Parameter / Policy | Setting |
|---|--|
| Unauthorized passwords: Users may not choose a password that matches or resembles the word “password” in any form (e.g. capitalized, adding a number) Users may not choose a password that pertains in any way to their name in any form (e.g. login name, first or last name) Password uniqueness must be maintained (no use of near-identical passwords) | Check <u>Disallow User Name?</u> Check <u>Disallow User ID?</u> Check <u>Disallow In Dictionary?</u> Add “password” variants to password dictionary |
| Inactive accounts disabling: Accounts showing no activity shall be disabled 90 days following password expiration. | Not available – must be reviewed manually |

Some attribute settings available in Tivoli Identity Manager Express:

- erPosixMaxPwdAge – maximum password age allowed
- erPosixMinPwdAge – minimum password age allowed
- erPosixPwdWarnAge – age of password before a warning is sent to the user about password expiration
- erPosixIdleDays – maximum number of days an account may remain idle before suspension
- erPosixPwdMaxAge – maximum amount of time a password remains valid after the maximum password age
- erPosixRloginRetries – maximum number of retries allowed when logging in
- erPosixPwdMinAlphaChar – minimum number of alphabetic characters in password
- erPosixPwdMinDiff – minimum difference between passwords
- erPosixPwdMinLen – minimum password length
- erPosixPwdCheck – specifies whether or not to check the password in a dictionary
- erPosixPwdDiction – specifies the dictionary files to check for the password
- erPosixPwdHistory – number of passwords to be remembered
- erPosixPwdHistoryExpire – number of weeks that must pass before the history is erased

Missing components: special character requirement and/or upper/lowercase requirement

A.7 Cisco Routers Versions: Cisco Secure ACS Appliance 3.2

| Parameter / Policy | Setting |
|--|---|
| Complexity: Systems shall enable automatic verification of passwords by the system. Passwords must contain three of the four following criteria: <ul style="list-style-type: none"> • English uppercase letters (A-Z) • English lowercase letters (a-z) • Westernized Arabic numerals (0-9) • Non-alphanumeric special characters (!, @, #, \$, &, *) | System Configuration > Local Password Management Select the Password must be alphanumeric check box |
| Minimum password length: Eight (8) characters | System Configuration > Local Password Management In Password length between X and Y characters, type the <i>minimum</i> valid number of characters for a password in the X box |

| Parameter / Policy | Setting |
|---|---|
| Expiration date: 90 days (85 days if grace period is available) | Select Apply age-by-date rules Set Active Period to 80 days Set Warning Period to 5 days |
| Grace period: (if available) 5 days | Select Apply age-by-date rules Set Grace Period to 5 days |
| Maximum number of consecutive unsuccessful login attempts: After three (3) unsuccessful login attempts in a row, the account shall be locked | In “User Setup Edit” choose Disable account if option Choose Failed attempts exceed and type in 3 |
| Lockout Duration: 30 minutes | Not available – accounts must be locked indefinitely until an administrator unlocks the account |
| Minimum password age: 5 days | Not available |
| Password reuse: Users may not use their previous five (5) passwords Users may not reuse a password within the past year | System Configuration > Local Password Management Select the Password is different from the previous value check box Will not provide a history of five passwords |
| Unauthorized passwords: Users may not choose a password that matches or resembles the word “password” in any form (e.g. capitalized, adding a number) Users may not choose a password that pertains in any way to their name in any form (e.g. login name, first or last name) Password uniqueness must be maintained (no use of near-identical passwords) | System Configuration > Local Password Management Select the Password may not contain the username check box |
| Inactive accounts disabling: Accounts showing no activity shall be disabled 90 days following password expiration. | Not available – must be reviewed manually |

A.8 OpenVMS

| Parameter / Policy | Setting |
|--|--|
| Complexity: Systems shall enable automatic verification of passwords by the system. Passwords must contain three of the four following criteria: <ul style="list-style-type: none"> English uppercase letters (A-Z) English lowercase letters (a-z) Westernized Arabic numerals (0-9) Non-alphanumeric special characters (!, @, #, \$, &, *) | Passwords are case insensitive, but may contain letters, numbers, underscore, and dollar sign. In order to enforce complexity, OpenVMS requires the creation and installation of a site-specific password filter that checks the existence of letters, numbers, and special characters within the password. |
| Minimum password length: Eight (8) characters | SET ACCOUNT POLICY/PASSWORD_POLICY=MINLENGTH=8 |
| Expiration date: 90 days (85 days if grace period is available) | SET ACCOUNT POLICY/PASSWORD_POLICY=MAXAGE=90 |
| Grace period: (if available) 5 days | Not available |
| Maximum number of consecutive unsuccessful login attempts: After three (3) unsuccessful login attempts in a row, the account shall be locked | SET ACCOUNT POLICY/LOCKOUT=ATTEMPTS=3 |
| Lockout Duration: 30 minutes | SET ACCOUNT POLICY/LOCKOUT=DURATION=30 SET ACCOUNT POLICY/LOCKOUT=WINDOW=30 |

| Parameter / Policy | Setting |
|---|--|
| Minimum password age: 5 days | SET ACCOUNT POLICY/PASSWORD_POLICY=MINAGE=5 |
| Password reuse: Users may not use their previous five (5) passwords Users may not reuse a password within the past year | SET ACCOUNT POLICY/PASSWORD_POLICY=HISTORY=5 \$ DEFINE/SYSTEM/EXEC SYS\$PASSWORD_HISTORY_LIFETIME 100 |
| Unauthorized passwords: Users may not choose a password that matches or resembles the word “password” in any form (e.g. capitalized, adding a number) Users may not choose a password that pertains in any way to their name in any form (e.g. login name, first or last name) Password uniqueness must be maintained (no use of near-identical passwords) | Create list of unauthorized passwords via: \$ CREATE LOCAL_PASSWORD_DICTIONARY.DATA Merge this list with existing password library using: \$ SET PROCESS/PRIVILEGE=SYSPRV \$ CONVERT/MERGE/PAD LOCAL_PASSWORD_DICTIONARY.DATA - _\$ SYS\$LIBRARY:VMS\$PASSWORD_DICTIONARY.DATA |
| Inactive accounts disabling: Accounts showing no activity shall be disabled 90 days following password expiration. | Not available – must be reviewed manually |

ATTACHMENT B: Password Parameter Compliance Matrix

This Page Intentionally Left Blank

Password Parameter Compliance Matrix

The below matrix details the capabilities of the listed operating systems to comply with the password parameter policies. Unenforced policies must be compensated by appropriate security countermeasures.

| Operating System | Complexity | Length | Expiration | Grace Period | Retries | Lockout Duration | Min. Age | Reuse | Unauth. Passwords | Disable Inactive |
|----------------------|------------|--------|------------|--------------|---------|------------------|----------|-------|-------------------|------------------|
| Windows | ● | ● | ● | N/A | ● | ● | ● | ● | ● | ○ |
| RACF | ○ | ● | ● | N/A | ● | ○ | ● | ● | | ● |
| Oracle (Database) | ● | ● | ● | ● | ● | ● | ○ | ● | ● | ○ |
| Oracle (Application) | ● | ● | ● | N/A | ● | ○ | ○ | ● | ● | ○ |
| Solaris | ○ | ● | ● | ● | ● | ○ | ● | ● | ● | ● |
| Tivoli | ○ | ● | ● | N/A | ● | ○ | ○ | ● | ● | ○ |
| Cisco | ● | ● | ● | ● | ● | ○ | | ● | ● | ○ |
| OpenVMS | ○ | ● | ● | N/A | ● | ● | ● | ● | ● | ○ |

● = Capable of enforcing parameter

○ = Capable of partially implementing parameter

ATTACHMENT C: Table of Applicable Accepted Risks

This Page Intentionally Left Blank

Table of Applicable Accepted Risks

The below table lists Federal Student Aid Accepted Risks related to password parameters. The table lists the finding number and its associated technology. To view the entire accepted risk, contact the corresponding System Security officer, or the Federal Student Aid Chief Security Officer.

| Finding Number | Technology |
|--------------------------------------|-------------------------------|
| OIGFY04FISMA-SC-44 | OpenVMS |
| FSA-VDC-CRG04-VS-0078 | Rational |
| FSA-VDC-OIGFY04FISMA-SC-64 | RACF |
| FSA-VDC-OIG-FY05-FISMA-0012 | (Unknown) |
| FSA-VDC-OIG-FY05-FISMA-0097 | Servers providing FTP service |
| FSA-FMS-INT-05-0001 | Oracle |
| FSA-FMS-INT-05-0002 | Oracle |
| FSA-FMS-INT-05-0003 | Oracle |
| FSA-FMS-INT-05-0004 | Oracle |
| FSA-FMS-INT-05-0005 | Oracle |
| FSA-FMS-INT-05-0006 | Oracle |
| FSA-ARS-APP-FY06-0001 | Oracle |
| COD-OIGFY04FISMA-SC-13 / COD-P-04-05 | Oracle |
| COD-OIGFY04FISMA-SC-14 | Oracle |
| FSA-COD-CRG04-VS-0022 | Oracle |
| FSA-COD-CRG04-VS-0023 | Oracle |
| FSA-COD-CRG04-VS-0024 | Oracle |
| FSA-COD-CRG04-VS-0025 | Oracle |
| FSA-COD-CRG04-VS-0026 | Oracle |
| FSA-COD-CRG04-VS-0027 | Oracle |
| FSA-COD-CRG04-VS-0028 | Oracle |
| FSA-COD-CRG04-VS-0029 | Oracle |
| | |